IL 01/13

PCT/IL 01/00013

31 JAN 2001

REC'D 12 FEB 2001

WIPO PCT

PA 352651

THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

January 16, 2001

4

THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM THE RECORDS OF THE UNITED STATES PATENT AND TRADEMARK OFFICE OF THOSE PAPERS OF THE BELOW IDENTIFIED PATENT APPLICATION THAT MET THE REQUIREMENTS TO BE GRANTED A FILING DATE UNDER 35 USC 111.

APPLICATION NUMBER: ***60/195,032***
FILING DATE: ***April 06, 2000***

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

By Authority of the
COMMISSIONER OF PATENTS AND TRADEMARKS

H. L. JACKSON
Certifying Officer

4-7-00 A/PROV

PROVISIONAL PATENT APPLICATION TRANSMITTAL

This is a request for filing a [illegible]ISIONAL APPLICATION under 37 CFR 1.53(b)(2).

Docket Number	NDS-4400 USA (P-066)	Type a plus sign (+) inside this box ->	+

INVENTOR(s)/APPLICANT(s)	
FIRST NAME, MIDDLE INITIAL, LAST NAME	RESIDENCE (CITY AND EITHER STATE OR FOREIGN COUNTRY)
1. Eli Hibshoosh	c/o NDS Technologies Israel Ltd., 5A Hamarpe Street, Har Hotzvim, P.O.Box 23012, Jerusalem 91235, ISRAEL
2. Chaim D. Shen-Orr	c/o NDS Technologies Israel Ltd., 5A Hamarpe Street, Har Hotzvim, P.O. Box 23012, Jerusalem 91235, Israel

TITLE OF THE INVENTION (280 characters max)

SECURE DIGITAL TO ANALOG CONVERTER

CORRESPONDENCE ADDRESS

Joel G. Ackerman
Limbach & Limbach L.L.P.
2001 Ferry Building
San Francisco
Phone: 415/433-4150; Fax: 415/433-8716

STATE	CA	ZIP CODE	94111-4262	COUNTRY	U.S.A.

ENCLOSED APPLICATION PARTS *(check all that apply)*

x	Specification *Number of Pages*	3			Small Entity Statement
x	Drawing(s) *Number of Sheets*	1			Other (specify):

METHOD OF PAYMENT *(check one)*

x	A check or money order is enclosed to cover the Provisional filing fees.	PROVISIONAL FILING FEE AMOUNT(S)	$150.00
X	The Commissioner is hereby authorized to charge any additional filing fees and credit Deposit Account Number: 12-1420		

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government

☐ No.

☐ Yes, the name of the U.S. Government agency and the Government contract number are:

Respectfully submitted,

SIGNATURE: [signature] Date: April 6, 2000

TYPED or PRINTED NAME: Joel G. Ackerman REGISTRATION NO. *(if appropriate)*: 24,307

CERTIFICATION UNDER 37 CFR §1.10

I hereby certify that this New Provisional Application and the documents referred to as enclosed herein are being deposited with the United States Postal Service on this date April 6, 2000, in an envelope bearing "Express Mail Post Office To Addressee" Mailing Label Number EL254108403US addressed to: Box Provisional Patent Application, Assistant Commissioner for Patents, Washington, D.C. 20231.

SIGNATURE: [signature] LANA T. BRENNER Date:

Secure Digital to Analog Converter (I-229)

Inventors: Eli Hibshoosh of Tel-Aviv, Israel, and Chaim D. Shen-Orr of Haifa, Israel.
Date: March 24 2000

Background

Digital Copy Protection implies an ability to control recording (prevent unauthorized copying) of any clear – decrypted - digital signal. Often the "clear" digital signal is converted to analog form without adequate protection as explained below.

Various methods may be used to encrypt the digital music content, ensuring that all decrypted (clear) signals are handled internally to the player device. However, technological advances available to copyright violators (hackers) make it imperative to avoid having clear digital content on any lines that go out of a secure piece of silicon.

The current main obstacle to achieving this goal stems from the current state of technology: High quality music reproduction, for example, requires at least 24-bit resolution Digital to Analog Converters (DACs). Real-time decryption and decoding of encrypted compressed music files requires high processing power CPU (Decryption / Decompression Engine – DDE). Placing the two together on a single piece of silicon results in coupling DDE electrical noise into the DAC analog output to a degree that results in unacceptable audio quality.

For this reason, all high-quality DACs are built into chips (integrated circuits) that are physically separate from the high-speed CPU's. The result is that lines from DDE's to DACs carry clear digital content data, e.g., corresponding to the audio. That point can be "sniffed" to extract the clear digital data.

The present invention is intended to circumvent the technology barrier described and create a Secure Digital to Analog Converter (SDAC). With such a device, any "sniffing" of the digital line / lines between the two components will yield commercially unusable noise or severely distorted signal.

Digital to Analog Converter background.

One form of conventional DAC (four-bit in fig. 1) is made out of resistors and resistor ladder elements (branches), to each of which a reference voltage is applied through an electronic switch. Each branch output voltage is zero if the corresponding switch is open, and a certain (fixed) value in case it is closed. These voltages are summed in an amplifier to produce the DAC output voltage.

A DAC also includes a digital interface – parallel or serial, in any of several standard formats - that accepts digital values to be converted. An input digital value is defined by a number of binary digits (bits), each of which may be either "0" or "1". The input interface electronics directs each of these bits to the appropriate switch.

The resistors are adjusted so that each branch produces a binary-weighted voltage value corresponding to the binary position of the bit that actuates the branch's switch. Thus the sum of

these voltages seen at the output amplifier is equal to a reference voltage times the input digital value.

Conventionally, the relative "weights" of the various bits (i.e. switch / resistors combination) of a DAC correspond to integral powers of two. That makes the output voltage value correspond exactly to the input binary word, except for the effects of (unwanted) non-linearities, noise and other undesirable effects. Thus, the ideal analog output voltage value corresponding to a N-bit digital input X is $Vref * \Sigma_i \{2^{-i} * X_i\}$, where i is the position of binary digit within the input word (from 1 to N), Xi is the value of the i-th binary digit (0 or 1), and Vref is the DAC reference voltage. This input/output relationship is known, linear and constant.

Non-linear DACs exist for special applications such as extending the output range without loss of resolution over a limited sub-range. In such DACs the relationship between the digital input word and the voltage output follows a non-linear function, but that function is known and constant, and in line with required accuracy.

Another conventional DAC form is the "one-bit" DAC, or more accurately "delta-sigma modulator with one bit DAC", which produces an analog voltage value by generating a high-frequency waveform whose instantaneous values are either of two known fixed numbers. These numbers ("step-up" and "step down"), are conveniently designated "0" and "1", but quite often are opposite-polarity, equal-amplitude values. The waveform averages, through a suitable filter, to the required instantaneous voltage.

To reduce DAC output noise it is important to keep the number of high-speed switches within the converter chip to a minimum, and have the necessary switching done in a synchronous manner. Similar considerations apply when the digital input to the DAC chip is serial rather than the parallel scheme just described.

Description of the invention.

The present invention attempts to create a Secure Digital to Analog Converter (SDAC) by combining three different ideas, none of them having been applied to this field before:

1. Implementing a CPU / crypto engine ("DACC") in the DAC chip and using it in low speed (or not at all) during the digital to analog conversion. CPU-related noise effects on DAC performance are therefore eliminated.

2. Constructing the DAC itself so that its input-output transfer function is settable by the DACC. The settings are so designed that there is no (or minimal) asynchronous switching during use. The variety of settings is such that it would be extremely difficult to extract the original (binary-weighted) digital word corresponding to an output voltage, given a limited number of observed SDAC digital inputs and analog output voltage measurement.

3. Establishing a "secure authenticated channel" between the DACC and the DDE by cryptographic means, during a short "setup session" at the beginning of a playout period (Figure 3). No content is played during the setup session, so the DACC can be in full operation and negotiate the transfer function parameters for the upcoming playout period

without any noise effect on the DAC when it is performing its main function of digital to analog conversion. Conversely, full-speed DACC operation is not required during the playout period, per (2) above.
Note that the secure authenticated channel and the digital signal channel (shown separately in Figure 3) may actually share the same physical lines.

Preferred embodiments

Starting with a setup session, a secure channel is established by any common cryptographic means, such as those used to communicate between any two secure devices. Typically, the channel will be initiated by the DDE.
Once a secure channel is established, the DACC will propose a randomly selected set of SDAC parameters. Once accepted, both sides will use the same set to achieve an overall linear transfer function.
On the source side (the DDE), these parameters will be used to modify the binary words transmitted to the SDAC for playout. The modification may be carried either in the DDE software (DAC driver) or in special-purpose hardware, or a combination of both.
On the receiving side (the SDAC), the DACC sets registers to control DAC operation, and than effectively shuts itself off. Alternatively, it may go into a reduced mode of operation so that its spurious (noise) effects on the DAC are within acceptable limits.
The DAC Control registers may affect DAC operation in any of the following, combinations, and variations:

A. Shuffle the bit order of the input word. For a 24-bit DAC, the number of combinations is on the order of 10^{23}.
B. Use non-binary weighted resistor values (Fig. 2) to create non-linear converter bit "weights". It should be noted that since the binary weight scheme is the most efficient, the number of bits in the non-binary-weighted converter must be increased to cover the same range. At the same time, rather small deviations from correct binary weights (due to resistor R2 in the example given) may cause enough distortion to make the content commercially unusable. Small deviations lead to a small number of additional bits required, and minimize requirements on deviation resistor / switch.
C. Use simple cryptographic functions that may be achieved by any number of means that do not impose excessive noise on the analog output. For example – XOR with the output of a Linear Feedback Shift Register.

Note that the invention is described in terms of a parallel DAC architecture. However, the same principle can be applied to any other DAC type. In particular, application of (B) to a one-bit DAC may be achieved by using unequal step-up and the step-down voltages.
Also, ancillary functions like calibration, control, inter-chip bus structure and standards, unprotected operation modes, and handling element inaccuracy have not been described.

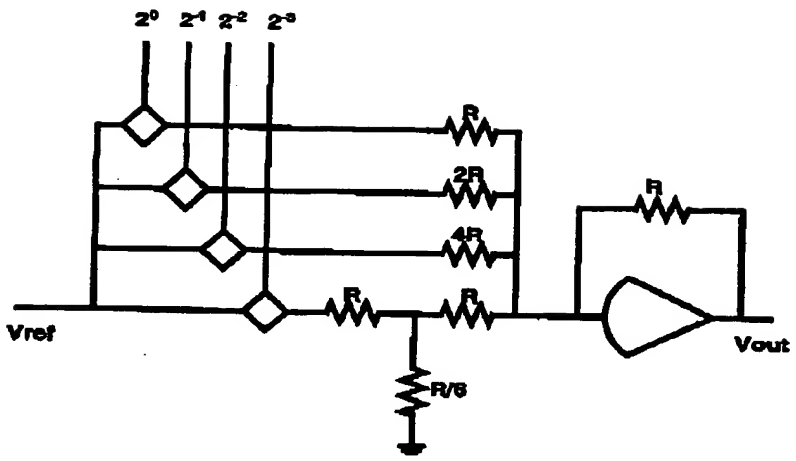

Figure 1

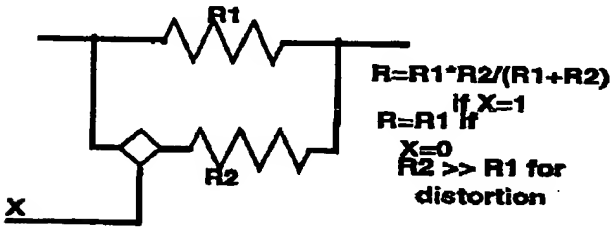

Figure 2

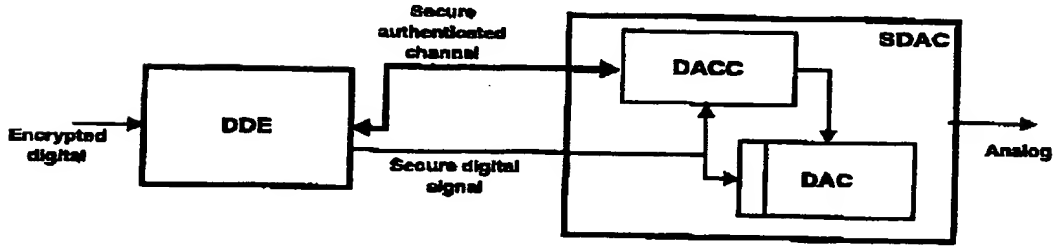

Figure 3